

AB:GK

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----- X

IN THE MATTER OF AN APPLICATION FOR A
SEARCH WARRANT FOR:

THE PREMISES KNOWN AND DESCRIBED AS
62-42 136th STREET, FLUSHING, NEW YORK,
11367

----- X

TO BE FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR A
SEARCH WARRANT

No. 19-M-295

EASTERN DISTRICT OF NEW YORK, SS:

AARON SPIVACK, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is kept and concealed within THE PREMISES KNOWN AND DESCRIBED AS 62-42 136th STREET, FLUSHING, NEW YORK, 11367 (the "PREMISES"), the items described in Attachment A to this affidavit, all of which constitute evidence or instrumentalities of the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, and the enticement of a minor, in violation of Title 18, United States Code, Sections 2252, 2252A (possession, receipt, and distribution of child pornography), and 2422 (coercion and enticement of minors) (the "Subject Offenses").

The source of your deponent's information and the grounds for his belief are as follows:¹

1. I have been a Special Agent of the FBI since October 2008, and am currently assigned to the New York Office. Since May 2010, I have been assigned to the Violent Crimes Against Children Task Force. I have been assigned to investigate violations of criminal law relating to the sexual exploitation of children. I have gained expertise in this area through training in classes and daily work related to conducting these types of investigations. As part of my responsibilities, I have been involved in the investigation of numerous child pornography cases and have reviewed hundreds of thousands of photographs depicting children (less than eighteen years of age) being sexually exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor. I am also a member of the Eastern District of New York Project Safe Childhood Task Force.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: my own personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography. Additionally, all statements attributable to individuals herein are set forth in sum and substance and in part.

¹ Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

3. The FBI is investigating possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, and the enticement of a minor, in violation of Title 18, United States Code, Sections 2252, 2252A (possession, receipt, and distribution of child pornography), and 2422 (coercion and enticement of minors).

I. DEFINITIONS

4. For the purposes of the requested warrant, the following terms have the indicated meaning in this affidavit:

- a. The terms “minor,” “sexually explicit conduct” and “visual depiction” are defined as set forth in Title 18, United States Code, Section 2256.
- b. The term “child pornography” is defined in Title 18, United States Code, Section 2256(8) in pertinent part as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. . . .”²
- c. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, server computers, and network hardware, as well as wireless routers and other hardware involved in network and Internet data transfer.
- d. The term “IP Address” or “Internet Protocol Address” means a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from

² See also Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static — that is, long-term — IP addresses, while other computers have dynamic — that is, frequently changed — IP addresses.

- e. The term “Internet” refers to a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- f. The term “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

II. BACKGROUND

A. PEER TO PEER FILESHARING

5. Peer to peer file sharing (“P2P”) is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on that network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user’s computer, and conducting searches for files that are currently being shared on another user’s computer.

6. The latest evolution of P2P software is a program that allows a user to set up his own private P2P network of contacts. File sharing through this new and publicly available P2P file sharing program is limited only to other users who have been added to a

private list of “friends.” A new user is added to a list of friends by request. Acceptance of a friend request will allow that new user to download files from the user who sent the friend request. The new user can then browse the list of files that the other user has made available to download, select desired files from this list, and download the selected files. The downloading of a file occurs through a direct connection between the computer requesting the file and the computer containing the file.

7. One aspect of P2P file sharing is that multiple files may be downloaded in parallel, which permits downloading more than one file at a time.

8. A P2P file transfer is assisted by reference to an IP address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

9. Third party software (“Network Monitoring Program” or “Investigative Software”) is available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet and local network traffic.

B. THE INVESTIGATION

10. In or around February, 2019, a law enforcement undercover agent associated with the Violent Crime Against Children Task Force who was working in an undercover capacity (“Undercover Officer”) signed into a publicly available peer-to-peer (P2P) program via an internet-connected computer. The Undercover Officer observed that P2P user “Sega628” was online and had folders containing child pornography files available for others to view and download. The Undercover Officer was not in a position to download

the child pornography files at the time, but noted Sega628's account on the P2P site for a future undercover session.

11. A different FBI undercover agent (UC-1) subsequently sent Sega628 a "friend" request, which Sega628 accepted on or about March, 01, 2019. UC-1 noted that according to the P2P "last login" information for Sega628, Sega628 primarily was logged into the P2P program late at night and/or on weekends. UC-1 sent Sega628 a message that stated, in sum and substance, "Hey man not sure how pervy you are. If you are a perv id love to chat. I'm a dad in ny/usa and pervy as fuck. hit me on kik if you want im 'steavantly'".

12. The application referenced by UC-1, Kik Messenger ("KIK"), is a mobile application similar to text messaging service which allows users to send messages as well as image and video files over cellular and wireless networks. Since the application is mobile, it granted UC-1 flexibility to communicate with Sega628 separate and apart from the P2P program and during off-hours and over weekends.

13. On or about March, 7, 2019, UC-1 received a KIK message from Sega628 that stated, in sum and substance, "You gave me your name through [the P2P program]." Sega628 stated that he was interested in "hard core young diapers and spanking". Sega628 additionally stated that he had a lot of "pics and videos." Sega628 asked about UC-1's children. In response, UC-1 stated, in sum and substance, that he had an eight-year-old boy and a ten-year-old girl, and that his girlfriend had a three-year-old child, all of whom UC-1 had sexually abused.

14. On or about March, 11, 2019, UC-1 asked Sega628 if he ever traded on the P2P program. Sega628 stated that he would log in so that UC-1 could download some of Sega628's files. Sega628 further explained that other than KIK, which was on his phone, "everything else is on my external that's hooked up to my laptop."

15. A few minutes later on or about March 11, 2019, UC-1 logged into his P2P account and downloaded approximately 116 image and video files from Sega628's account, the vast majority of which consist of child pornography and child erotica. Some of the files downloaded by UC-1 are described as follows:

- a. "x_59a98225" is an image depicting a prepubescent girl under the approximate age of 10 lying face down on a couch and nude from the waist down. The child's hands are bound behind her back with what appears to be duct tape and her legs are forced apart with rope and what appears to be duct tape, exposing her genitals.
- b. "03-004-02 JudyAn set 04 Make it Big" is a video, approximately 56 seconds in length, which depicts a fully nude prepubescent girl under the approximate age of 12 rubbing the erect penis of an adult man which is pressed into the child's vagina.

Sega628 stated that his shared drive contained "anywhere from fifty to a hundred gigs" of material in total.

16. Later during the chat on or about on or about March 11, 2019, Sega628 asked what UC-1 had done to his children sexually. Sega628 stated that he wanted to "spank the 3 year old." Sega628 requested photographs of UC-1's children, after which UC-1 sent

several images which he claimed depicted his eight-year-old son and ten-year-old daughter. In response, Sega628 stated, “dam they are so hot and cute this just me a big boner.”

17. Sega628 stated that he was interested in meeting with UC-1. Sega628 provided that his name is “Steven;” that he is 32 years of age (turning 33 in June), that he lives in Flushing, Queens; and that he works with his father on “a big construction project.”

18. On or about March, 15, 2019, Sega628 contacted UC-1 on KIK and asked if UC-1 was around to download more of Sega628’s P2P files. UC-1 logged in and downloaded approximately 86 image and video files. With the exception of a few animated images, the files consistent entirely of child pornography and child erotica. Some of the files downloaded by UC-1 are described as follows:

a. “Best 1 yo baby kim” is a video, approximately 42 seconds in length. The video depicts a fully nude female child, approximately under the age of 2. An adult male rubs his erect penis around the child’s vagina and engages the child in oral sex.

b. “41619248SHb” is an image depicting a prepubescent child under the approximate age of 12 who is nude from the waist down. The child is lying on her back with her legs in the air exposing her vagina and anus. Inserted into the child’s anus is what appears to be a marker.

19. Sega628 subsequently requested additional photographs of UC-1’s children. UC-1 sent Sega628 an additional image which appears to depict a young child who UC-1 stated was his daughter. Sega628 responded that he “would love some nude shots of them.” Sega628 then stated that his parents would be out of town the week of April 2, 2019

and that he would like to meet up with UC-1 and his children. Sega628 advised that he wanted to “spank and fuck both of your kids” as well as “share pics.”

20. Sega628 then sent UC-1 a link, containing approximately 223 video files all consistent with being child pornography. Some of the files downloaded and contained in the link are described as follows:

- a. “20150823_222735000_iOS” is a video approximately one minute and 23 seconds in length. The video depicts a prepubescent child under the approximate age of 12 engaging in oral sex with an adult male’s erect penis.
- b. “20150825_132447000_iOS” is a compilation video approximately one minute and 31 seconds in length. The video depicts multiple prepubescent children engaged in various sexual acts including vaginal penetration, oral sex, anal sex and genital exposure.

21. On or about March 18, 2019, Sega628 and UC-1 communicated again on KIK. Sega628 asked if UC-1’s girlfriend’s three-year-old child was still in diapers. Sega628 then sent UC-1 another link which Sega628 stated contained “about a hundred spanking videos.” UC-1 downloaded the link which contained approximately 100 videos of children being spanked. Some of these videos depict the children nude and/or partially nude. Sega628 then requested UC-1 to send him “nude and or ass shot” of UC-1’s children and provided that he is “very much into asses and spanking.”

22. On or about March, 28, 2019, Sega628 contacted UC-1 via KIK and asked UC-1 to send him photographs of UC-1’s children and explained, “if you can arrange

and get them I want to see their face and body and ass all in there underwear and sexy positions.”

23. On or about March, 28, 2019, Sega628 asked UC-1 via KIK, “did you do anything fun with your kids last night”. UC-1 responded, “just a little touching.” Sega628 then suggested, “you should plan a daddy fun day next week so I can have fun with them like we discuss[ed]” and noted that he was free Wednesday through Friday of the week of April 1, 2019.

24. UC-1 sent Sega628 additional photographs that he claimed depicted his children. With regard to a photograph depicting UC-1’s purported son, Sega628 stated, “I wish you had pull the underwear in the middle so i could see the ass checks.” Sega628 also commented on the image depicting UC-1’s purported daughter and stated, “wow she is hot how do you control yourself around her” and “I love her nice small ads [sic] and her leg...ass.”

25. UC-1 asked Sega628 which of the children Sega628 wanted to “play with” when they met. Sega628 stated, “Your daughter mainly after seeing her,” and, “Really all 3, but I want her now.”

26. UC-1 and Sega628 initially discussed meeting at UC-1’s residence in Manhattan, New York. However, Sega628 later suggested meeting at his residence instead and stated that he lives in an “empty private home so we could do more without worrying about the neighbors if you bring your kids over to me” and that he has “a nice big basement with the recliner so you can sit back and watch while I have fun with your kid.”

27. On or about March 29, 2019, UC-1 and Sega628 communicated again via KIK and made arrangements to meet up with UC-1's daughter on Wednesday, April 3, 2019, at Sega628's residence. Sega628 asked, "what are my limits what can I do and not do with your daughter," and stated, "I want to spank her play with her ass and pussy and fuck her." Sega628 later explained "[t]he [first] thing I am[going to do] is strip[] her nude the[n] lightly spanking her with a small slipper I have [until] she is crying and her ass is red do not worry I will not bruise her ... Then I am going to finger her ass and pussy ... Then I will drug her and fuck her."

28. Sega628 stated that he would buy UC-1's daughter Haribo gummy bears as a gift, and that he had "lube and condoms" and that would also get sleeping medication, "Zzz quill."

29. During their communication, Sega628 informed UC-1 that his home address is 6242 136th Street, Flushing, NY 11367. Sega628 stated the house has no additional occupants beyond him and members of his family.

30. Sega628 additionally informed UC-1 that his collection of child pornography is contained on an external hard drive that he plugs into his laptop computer and desktop computer. Sega628 stated that an "xxx folder" on the hard drive contains 246 gigabytes of data in total.

31. The FBI used the Network Monitoring Program to identify the IP address utilized by Sega628 when he was using the P2P program as 98.116.57.231. Through a subpoena to KIK, the affiant has learned that this was the same IP address used by Sega628

on KIK Messenger. Open source database searches revealed the IP address 98.116.57.231 was registered to Verizon Fios.

32. Records obtained from Verizon Fios by administrative subpoena showed that IP address 98.116.57.231 on February, 05, 2019 at 5:45PM ET was subscribed to Rodrigo Acosta, located at 62-42 136, Flushing, NY 11367, the PREMISES. Significantly, the address provided in response to the subpoena matches the address that Sega628 provided during his KIK chats with UC-1.

33. Open source database and website checks revealed that those residing at the PREMISES include Estavan Acosta, date of birth June, 28, 1986. Significantly, the month of birth and age obtained from such record checks match up with those provided by Sega628 during his KIK chats with UC-1. In addition, “Estavan” is Spanish for “Steven”—the name provided by Sega628 during his KIK chats.

III. CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

34. Based on my training and experience and conversations that I have had with other federal agents and law enforcement officers, I know that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so usually by ordering it from abroad or by discreet contact, including through the use of the Internet, with other individuals who have it available or by accessing web sites containing child pornography. Child pornography collectors often send and receive electronic mail conversing with other collectors in order to solicit and receive child pornography.

35. I know that collectors of child pornography typically retain their materials and related information for many years.

36. I also know that collectors of child pornography often maintain lists of names, addresses, telephone numbers and screen names of individuals with whom they have been in contact and who share the same interests in child pornography.

37. Accordingly, information in support of probable cause in child pornography cases is less likely to be stale because collectors and traders of child pornography are known to store and retain their collections and correspondence with other collectors and distributors for extended periods of time.

38. I also know that child pornography offenders are often recidivists, even while under supervision.

39. Based on my experience, I know that persons who collect and distribute child pornography frequently collect sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification.

40. Further, based on my training, knowledge, experience, and discussions with other law enforcement officers, I understand that, in the course of executing a search warrant for the possession, transportation, receipt, distribution or reproduction of sexually explicit material related to children, on numerous occasions officers have recovered evidence related to the production of child pornography and/or child exploitation.

IV. THE PREMISES

41. The PREMISES is one of two units of a standalone split-level house with an attached attic and basement, as well as a detached garage to the rear. The façade of the PREMISES is comprised of red brick and a white pane exterior with windows along the front and side. The entrance to the PREMISES is up a small set of stairs and through a white colored door with a glass window in the middle. Approaching the PREMISES on the street-facing exterior and to the left of the entrance are the numbers “62 42.” Along the side of the PREMISES is one utility reader, indicating the PREMISES is a single-family occupancy.





V. TECHNICAL BACKGROUND

42. As described above and in Attachment B, this application seeks permission to search for documents constituting evidence, fruits or instrumentalities of violations of Title 18, United States Code, Sections 2252, 2252A, and 2422 that might be found on the PREMISES, in whatever form they are found. One form in which the documents might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of computers and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure.

43. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they

have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers’ internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from the use of an operating system or application, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

e. Based on the evidence that a computer connected to a P2P network through an IP address registered at the PREMISES, there is reason to believe that there is a computer currently located on the PREMISES. Additionally, Sega628 stated to UC-1 that he uses a desktop computer to watch his child pornography collection and transfers files between his laptop and his desktop computer.

44. As further described in Attachment B, this application seeks permission to locate not only electronic computer files that might serve as direct evidence of the crimes described on the warrant, but also electronic “attribution” evidence that establishes how the computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer or storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, Internet search histories, configuration files, user profiles, email, email address books, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how the computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on a computer is evidence may depend on the context provided by other information stored on the computer and the application of knowledge about how a computer functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, it is sometimes necessary to establish that a particular item is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user’s intent.

45. In most cases, a thorough search for information that might be stored on computers and storage media often requires agents to seize such electronic devices and later review the media consistent with the warrant. This is true because of the time required for examination, technical requirements, and the variety of forms of electronic media, as explained below:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on-site. Analyzing electronic data for attribution evidence and conducting a proper forensic examination requires considerable time, and taking that much time on the PREMISES could be unreasonable. Given the ever-expanding data storage capacities of computers and storage media, reviewing such evidence to identify the items described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. The variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

46. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant sought would authorize seizing, imaging, or otherwise copying computers and storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

47. Because several people might share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is probable that the things described in this warrant could be found on any of those computers or storage media, the warrant sought would permit the seizure and review of those items as well.³

³ As a matter of practice, the FBI identifies electronic devices used as a means to commit violations of 18 U.S.C. §§ 2252, 2252A and 2422 based on the location of the electronic devices within the PREMISES as well as conversations with individuals present at THE PREMISES. If the electronic devices identified through such means do not contain evidence or instrumentalities of violations of Title 18, United States Code Sections 2252, 2252A, and 2422, additional electronic devices within THE PREMISES are identified through a cursory scan using a forensic program designed to identify records or information used as a means to commit violations of 18 U.S.C. §§ 2252, 2252A and 2422. If a device seized during a search warrant appears to belong to an innocent third party, the FBI releases the device as soon as the device has been imaged and has been confirmed to be “clean,” i.e.,

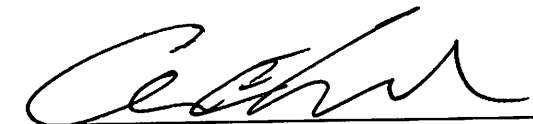
VI. CONCLUSION

48. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the PREMISES there exists evidence of crimes. Accordingly, a search warrant is requested.

49. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application and search warrant. I believe that sealing these documents is necessary because, given the confidential nature of this investigation, disclosure would severely jeopardize the investigation in that it might alert the target(s) of the investigation at the PREMISES to the existence of an investigation and likely lead to the destruction and concealment of evidence, and/or flight.

WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for THE PREMISES KNOWN AND DESCRIBED AS 62-42 136th STREET, FLUSHING, NEW YORK, 11367.

IT IS FURTHER REQUESTED that all papers submitted in support of this application, including the application and search warrant, be sealed until further order of the Court.



Special Agent Aaron E. Spivack
Federal Bureau of Investigation

does not contain any contraband or evidence of a crime. Until a given electronic device has been examined, there is no way to determine whether it was used to facilitate the criminal conduct under investigation or whether items relevant to the investigation have been transferred to such device.

Sworn to before me this
2nd day of April, 2019

THE HONORABLE ROANNE L. MANN
CHIEF UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A
Property to Be Searched

The property to be searched is 62-42 136th STREET, FLUSHING, NEW YORK, 11367 (the PREMISES) further described as one of two units of a standalone split-level house with an attached attic and basement, as well as a detached garage to the rear. The façade of the PREMISES is comprised of red brick and a white pane exterior with windows along the front and side. The entrance to the PREMISES is up a small set of stairs and through a white colored door with a glass window in the middle. Approaching the PREMISES on the street-facing exterior and to the left of the entrance are the numbers “62 42”. Along the side of the PREMISES is one utility reader, indicating the PREMISES is a single-family occupancy.





ATTACHMENT B
Property to be Seized

ITEMS TO BE SEIZED FROM THE PREMISES, all of which constitute evidence or instrumentalities of violations of Title 18, United States Code Sections 2252, 2252A, and 2422:

1. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A, in any form wherever they may be stored or found;
2. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
4. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
5. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:
 - a. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
 - b. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

6. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.
7. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
8. Records evidencing occupancy or ownership of the PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.
9. Records or other items which evidence ownership or use of computer equipment found in the PREMISES, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.
10. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct.
11. Address books, names, lists of names and addresses of individuals believed to be minors.
12. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be minors.
13. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.
14. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

15. Computers¹ or storage media² that contain records or information (hereinafter “COMPUTER”) used as a means to commit violations of 18 U.S.C. §§ 2252, 2252A and 2422. All information obtained from such computers or storage media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252, 2252A, and 2422, including:
- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - f. evidence of the times the COMPUTER was used;
 - g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

¹ A computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers, and network hardware, such as wireless routers.

² A “storage medium” for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - i. contextual information necessary to understand the evidence described in this attachment;
- 16. Records and things evidencing the use of the Internet Protocol address 24.102.95.184, including:
 - a. routers, modems, and network equipment used to connect computers to the Internet;
 - b. Internet Protocol addresses used by the COMPUTER;
 - c. records or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
- 17. Haribo gummy bears, stuffed animals, lubricant, condoms, sleep medication, and any similar items that potentially evidence the attempted enticement of a minor in violation of Title 18, United States Code, Section 2422.
- 18. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein, all of which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252, 2252A, and 2422.